PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: HARALD VATER ET AL
SERIAL NO.: 09/763,621
FILED: April 26, 2001
FOR: ACCESS-PROTECTED DATA CARRIER

GROUP ART UNIT: 2134
EXAMINER: C. Colin
ATTY. REFERENCE: VATE3002/BEU

COMMISSIONER OF PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The below identified communication(s) or document(s) is(are) submitted in the above application or proceeding:

- ☐ Declaration
- ☐ Priority Document
- ☐ Formal Drawings
- ☐ Assignment
- ☐
- ☐ Application Data Sheet
- ☒ **Request for Rehearing (in triplicate)**

☒ Please debit or credit **Deposit Account Number 02-0200** for any deficiency or surplus in connection with this communication. A duplicate copy of this sheet is provided for use by the Deposit Account Branch.

☐ Small Entity Status is claimed.

☐

23364
Customer Number

BACON & THOMAS, PLLC
625 SLATERS LANE - FOURTH FLOOR
ALEXANDRIA, VIRGINIA 22314
(703) 683-0500

DATE: January 16, 2007

Respectfully submitted,

Benjamin E. Urcia
Attorney for Applicant
Registration Number: 33,805

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of:	)	**Group Art Unit: 2134**
	)	
Harald VATER *et al.*	)	**Examiner: C. Colin**
	)	
Serial Number: 09/763,621	)	***Attorney Docket*: VATE3002beu**
	)	
Filed: April 26, 2001	)	**Confirmation No.: 8124**

For: Access-Protected Data Carrier

REQUEST FOR REHEARING UNDER 37 C.F.R. §41.52
(In Triplicate)

Sir:

This paper is an Request for Rehearing in reply to the Decision on Appeal dated May 13, 2008.

The Appellant believes that the following point raised in the Appeal Brief dated were overlooked or misapprehended by the Board:

- According to page 6 of the Appeal Brief,

> Reversal of the rejection under 35 USC §102(e) is respectfully requested on the grounds that the Kocher publication does not disclose or suggest, whether individually or in common with any other reference of record, a data carrier having a semiconductor chip with a memory and operating program that disguises an operation h and its input x in order to obtain a disguised operation h_{RI} ***different from operation h*** and disguised input data in which:
>
> $$\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$$
>
> holds true, *i.e.*, in which **performing the different operation on the disguised input data has the same effect as performing the original operation on the undisguised input data**, as recited in independent claim 1, or in which the result of performing the original operation on the undisguised input data can be determined from the output data with the aid of data used for the disguising the operation, as recited in second independent claim 9.

In the method of Kocher, the relationship $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$ does not hold true.

It appears that the Applicant's arguments concerning "disguising" of the operation have been mis-apprehended. The Board has apparently understood "disguising" to be equivalent to "modifying," which is not the case. The Applicant admits that Kocher modifies the DES algorithm. However, the Applicant does not admit that the modification results in the claimed equality $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$.

In hindsight, it appears that use of the term "standard DES" operation to describe Kocher's modified DES algorithm may have confused the Board (and the Examiner). It actually does not matter whether the DES operation described by Kocher should be considered to be "standard" or not. The critical point, which has been misapprehended or overlooked, is that Kocher does not seek to achieve the relationship $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$, and in fact does not require such a relationship. Just because Kocher modifies the "standard" DES algorithm does not mean that the result of applying of the modified DES algorithm to disguised input data (M1,M2 according to Kocher's terminology) is exactly equal, as claimed, to the result of applying the "standard" DES algorithm to the undisguised input data (M). To the contrary, there is no inherent reason why there should be any relationship between applying an encryption (or decryption) algorithm to data and applying a modified encryption (or decryption) algorithm to either the same data, a disguised version of the data, or entirely different data.

Kocher is not the only one to teach modifications to the DES algorithm, and it is hardly reasonable to expect that all of such modifications will obey the claimed equality. For example, as explained below, Kocher mentions that the modifications made to the DES algorithm (revised initialization procedures and added permutations) could also be applied to DES-X, or even to RSA. It is not reasonable to expect that the result of applying the revised DES-X or RSA algorithms to disguised data M1,M2 would be equal to the result of applying standard DES to original data M. Instead, the result will be different each time a modification is made to DES,

unless the modifications are specifically designed, as in the claimed invention, to obtain the same result, *i.e.*, the claimed equality $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$.

This is not a repeat of the arguments made in the Appeal Brief, but it also is not a new argument. It appears that there has been a mis-understanding of Applicant's arguments based on semantics (*i.e.*, unfortunately choice of terminology on the part of the undersigned, which seems to have caused confusion). In particular, Applicant's use of the term "standard" to describe Kocher's modified DES algorithm was unfortunate. Kocher in fact clearly does modify the DES algorithm, by varying the initialization process for the S tables and by adding permutations and varying the keys. What the Board/Examiner has overlooked, and the Appeal Brief apparently did not make completely clear, is that modifying is not the same as disguising.

The Applicant's "disguising" operation is actually a randomizing operation, and not just randomization by inputting random numbers. Applicant's "disguising: operation actually results in an operation that does not bear a predetermined relationship to the original operation, *which is why it is necessary that* $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$. If the claimed equality were not present, then it would be impossible (or at least extremely difficult) for a decrypter to recover the original data (or for en encrypter to encrypt the data in a way that could be recovered) because the operation used to encrypt the data has been "**disguised**" and **not merely modified**. This is a fundamental feature of the claimed invention, which relies on the lack of a predictable relationship between the original algorithm and the disguised algorithm to protect the original algorithm. Kocher's goal is completely different, namely to modify DES in such a way as to make it more difficult to detect *during execution*. Kocher does not seek to hide the manner in which the DES algorithm has been modified, and therefore does not require a relationship between the original and modified algorithms, as claimed.

What has been misapprehended is that the claimed "disguised operation" is not at all the same as Kocher's modified DES operation. While use of the term "disguised" might by itself

not distinguish the claimed invention from a modified algorithm as taught by Kocher, the term "disguised" was intended to have an entirely different meaning than "modified." The difference is that a disguised operation cannot be reversed, with the result that it is necessary to impose an additional equality, namely that $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$, which is not at all necessary if the operation is merely modified as in Kocher.

The claimed invention has two aspects: a. disguising of data; and b. disguising of operations to be performed on the data. The Kocher publication clearly teaches disguising of input data and keys (see paragraphs [0033] to [0037]), and in fact uses the same disguising operation as Applicant. In particular, input data M is disguised by X-ORing with a random number to obtain M1 and M2 (M1 is the random number and M2 is the X-OR'd random number). Key K is also disguised by X-ORing with a random number. This is the same basic process as is used by the present invention to disguise the input data (both the "message" and the "keys" are input data).

Further, it is absolutely true that Kocher teaches ***modifications*** to the DES algorithm. These modifications involve improving the manner in which the S tables are initialized and updated so that the table entries can be changed more frequently (preferably the table entries are changes faster than they can be discovered by an attacker), as described in paragraphs [0039] to [0051]. In addition,"improvements" or modifications to the DES algorithm are described in paragraphs [0052] to [0064]. These modifications involve adding permutations, such as the PC2 operation in paragraph [0054], which is apparently a departure from the "standard DES PC1 operation" described in the first sentence of the paragraph. The result is a modified DES algorithm which has harder-to-discover random number inputs, resulting from improved *initialization* of the S tables, and more permutations (both in quantity and complexity).

The fact that Kocher modifies the DES algorithm, for example by constantly updating the S tables that supply random numbers to the algorithm, in order to keep ahead of an attacker, does not imply that $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$. The reason is as follows: The claimed

invention assumes that the operation used to carry out the encryption will be discovered by an attacker, but seeks to protect the data by using an operation h' whose relationship to the original operation h is random, except that $\mathbf{h_{RI}}$**(disguised input data) = y = h(x)**. If the relationship between disguised input data and the original data is not known, then the relationship between h' and h also cannot be discovered. This lack of a predetermined relationship between h' and h, which is what is meant by the term "disguising," has the effect of completely protecting h and x, but also would have the effect of making it impossible to recover the original data even for legitimate reasons if it were not for the claimed relationship $\mathbf{h_{RI}}$**(disguised input data) = y = h(x)**. On the other hand, by forcing h' to comply with the relationship $\mathbf{h_{RI}}$**(disguised input data) = y = h(x),** the original data can be recovered without any knowledge of h' at all.

In contrast, Kocher seeks to keep one step ahead of the attacker by varying the various random numbers used in the DES algorithm and adding permutations, and does not seek to disguise the relation between the modified DES algorithm and the so-called "standard DES algorithm." Instead, Kocher assumes that someone seeking to recover the original data can do so in the usual manner, but simply reversing the algorithm applied to the disguised data using secret keys, and then recovering the original data using additional keys (the random numbers used to disguise the data). Kocher does not need the claimed equality (*i.e.*, h_{RI}(disguised input data) = y = h(x)) because, although the "standard" DES algorithm is changed or modified to include different initialization and additional permutations, the DES algorithm is not changed in a random manner. So long as the decryption algorithm used to recover the original data takes into account the modifications made by Kocher to the DES encryption algorithm, there is no need for the claimed equality to hold true.

The logical error made by the Examiner is to assume that the result of encrypting the disguised data using a modified algorithm must equal the result of encrypting the original data using the original algorithm. This is not the case. There are actually many variations of DES, such as DES-X mentioned in paragraph [0068] of the Kocher publication, any of which could be applied to the original or disguised data. There is no reason to assume that a file encrypted

by DES-X would be the same as a file encrypted by DES. If a particular file is encrypted by DES-X, then it must be decrypted by DES-X, and cannot be decrypted by basic DES. Similarly, a file encrypted by Kocher's modified DES, with its additional permutations, will need to be decrypted by a modified version of DES. This is entirely to be expected, and not normally a problem. One does not expect an RSA encrypted file to be identical to a DES encrypted file, and therefore decryptable by the same algorithm. Similarly, one does not expect an encrypted file that has been encrypted by modified DES file to be the same as a file encrypted by DES. The algorithms might be different, but one is not a "disguised" version of the other. So long as the decrypted knows how the file was encrypted, the file can be decrypted, no matter how good the protection against third party attackers. (Note that the same argument applies to decryption, which either requires knowledge of the encryption algorithm, or a decryption algorithm whose output is not affected by the specific algorithm employed, *i.e.*, that exhibits the claimed equality).

Even if one refers to the modified DES algorithm of Kocher as "h'", since h' is merely a modified version of h, someone practicing the teachings of Kocher can simply reverse h' to recover the original disguised data, *i.e.*, to decrypt the encrypted file, and then reverse the data disguising operation to recover the original undisguised data. That is not the case with the claimed invention. Instead, the encryption operation is itself randomized. This does not simply mean that random numbers are used in the operation. All major encryption algorithms use random numbers. Instead, it means that the operation itself has been **modified in a random way**. This is the fundamental difference between the claimed invention and what is taught by Kocher. **The claimed disguising of an operation is not merely modification of the operation (whether by modifying S tables, or adding permutations, or changing the keys), but rather involves a random modification of the operation, necessitating the claimed equality $E(x)_h = E(x')_{h'}$.**

The different nature of the claimed "disguising" of operations and Kocher's teachings concerning variations of the DES algorithm may be further understood from the fact that falsification of the encryption operations, according to the present invention, must be carried

out before execution, *i.e.*, in a safe environment, in order to be able to achieve the claimed equality (*i.e.*, it is necessary to run the disguised operations in order to generate a disguised operation that exhibits the claimed equality). While Kocher's DES modifications do involve initialization, the initialization *changes* each time the algorithm is run, and cannot be carried out in a safe environment by also running the original algorithm. To the contrary, running the unmodified DES algorithm on undisguised data would be contrary to Kocher's goal of varying the initialization or set-up each time a data encryption operation is to be performed and therefore Kocher could not have suggested that the claimed equality between a disguised operation applied to disguised data and an undisguised operation applied to undisguised data.

Conclusion

For all of the foregoing reasons, Appellants respectfully requested reconsideration of the Decision on Appeal, and reversal of final rejection of claims 1-18 under 35 U.S.C. §102(e).

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: July 14, 2008

BACON & THOMAS
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500

S:\Producer\beu\Pending Q...Z\V\VATER 763621\rehearing request.wpd

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of:	)	**Group Art Unit: 2134**
	)	
Harald VATER *et al.*	)	**Examiner: C. Colin**
	)	
Serial Number: 09/763,621	)	***Attorney Docket*: VATE3002beu**
	)	
Filed: April 26, 2001	)	**Confirmation No.: 8124**

For: Access-Protected Data Carrier

REQUEST FOR REHEARING UNDER 37 C.F.R. §41.52
(In Triplicate)

Sir:

This paper is an Request for Rehearing in reply to the Decision on Appeal dated May 13, 2008.

The Appellant believes that the following point raised in the Appeal Brief dated were overlooked or misapprehended by the Board:

- According to page 6 of the Appeal Brief,

> Reversal of the rejection under 35 USC §102(e) is respectfully requested on the grounds that the Kocher publication does not disclose or suggest, whether individually or in common with any other reference of record, a data carrier having a semiconductor chip with a memory and operating program that disguises an operation h and its input x in order to obtain a disguised operation h_{RI} ***different from operation h*** and disguised input data in which:
>
> $$\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$$
>
> holds true, *i.e.*, in which **performing the different operation on the disguised input data has the same effect as performing the original operation on the undisguised input data**, as recited in independent claim 1, or in which the result of performing the original operation on the undisguised input data can be determined from the output data with the aid of data used for the disguising the operation, as recited in second independent claim 9.

In the method of Kocher, the relationship $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$ does not hold true.

It appears that the Applicant's arguments concerning "disguising" of the operation have been mis-apprehended. The Board has apparently understood "disguising" to be equivalent to "modifying," which is not the case. The Applicant admits that Kocher modifies the DES algorithm. However, the Applicant does not admit that the modification results in the claimed equality $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$.

In hindsight, it appears that use of the term "standard DES" operation to describe Kocher's modified DES algorithm may have confused the Board (and the Examiner). It actually does not matter whether the DES operation described by Kocher should be considered to be "standard" or not. The critical point, which has been misapprehended or overlooked, is that Kocher does not seek to achieve the relationship $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$, and in fact does not require such a relationship. Just because Kocher modifies the "standard" DES algorithm does not mean that the result of applying of the modified DES algorithm to disguised input data (M1,M2 according to Kocher's terminology) is exactly equal, as claimed, to the result of applying the "standard" DES algorithm to the undisguised input data (M). To the contrary, there is no inherent reason why there should be any relationship between applying an encryption (or decryption) algorithm to data and applying a modified encryption (or decryption) algorithm to either the same data, a disguised version of the data, or entirely different data.

Kocher is not the only one to teach modifications to the DES algorithm, and it is hardly reasonable to expect that all of such modifications will obey the claimed equality. For example, as explained below, Kocher mentions that the modifications made to the DES algorithm (revised initialization procedures and added permutations) could also be applied to DES-X, or even to RSA. It is not reasonable to expect that the result of applying the revised DES-X or RSA algorithms to disguised data M1,M2 would be equal to the result of applying standard DES to original data M. Instead, the result will be different each time a modification is made to DES,

unless the modifications are specifically designed, as in the claimed invention, to obtain the same result, *i.e.*, the claimed equality $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$.

This is not a repeat of the arguments made in the Appeal Brief, but it also is not a new argument. It appears that there has been a mis-understanding of Applicant's arguments based on semantics (*i.e.*, unfortunately choice of terminology on the part of the undersigned, which seems to have caused confusion). In particular, Applicant's use of the term "standard" to describe Kocher's modified DES algorithm was unfortunate. Kocher in fact clearly does modify the DES algorithm, by varying the initialization process for the S tables and by adding permutations and varying the keys. What the Board/Examiner has overlooked, and the Appeal Brief apparently did not make completely clear, is that modifying is not the same as disguising.

The Applicant's "disguising" operation is actually a randomizing operation, and not just randomization by inputting random numbers. Applicant's "disguising: operation actually results in an operation that does not bear a predetermined relationship to the original operation, *which is why it is necessary that* $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$. If the claimed equality were not present, then it would be impossible (or at least extremely difficult) for a decrypter to recover the original data (or for en encrypter to encrypt the data in a way that could be recovered) because the operation used to encrypt the data has been "**disguised**" and **not merely modified**. This is a fundamental feature of the claimed invention, which relies on the lack of a predictable relationship between the original algorithm and the disguised algorithm to protect the original algorithm. Kocher's goal is completely different, namely to modify DES in such a way as to make it more difficult to detect *during execution*. Kocher does not seek to hide the manner in which the DES algorithm has been modified, and therefore does not require a relationship between the original and modified algorithms, as claimed.

What has been misapprehended is that the claimed "disguised operation" is not at all the same as Kocher's modified DES operation. While use of the term "disguised" might by itself

not distinguish the claimed invention from a modified algorithm as taught by Kocher, the term "disguised" was intended to have an entirely different meaning than "modified." The difference is that a disguised operation cannot be reversed, with the result that it is necessary to impose an additional equality, namely that $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$, which is not at all necessary if the operation is merely modified as in Kocher.

The claimed invention has two aspects: a. disguising of data; and b. disguising of operations to be performed on the data. The Kocher publication clearly teaches disguising of input data and keys (see paragraphs [0033] to [0037]), and in fact uses the same disguising operation as Applicant. In particular, input data M is disguised by X-ORing with a random number to obtain M1 and M2 (M1 is the random number and M2 is the X-OR'd random number). Key K is also disguised by X-ORing with a random number. This is the same basic process as is used by the present invention to disguise the input data (both the "message" and the "keys" are input data).

Further, it is absolutely true that Kocher teaches ***modifications*** to the DES algorithm. These modifications involve improving the manner in which the S tables are initialized and updated so that the table entries can be changed more frequently (preferably the table entries are changes faster than they can be discovered by an attacker), as described in paragraphs [0039] to [0051]. In addition,"improvements" or modifications to the DES algorithm are described in paragraphs [0052] to [0064]. These modifications involve adding permutations, such as the PC2 operation in paragraph [0054], which is apparently a departure from the "standard DES PC1 operation" described in the first sentence of the paragraph. The result is a modified DES algorithm which has harder-to-discover random number inputs, resulting from improved *initialization* of the S tables, and more permutations (both in quantity and complexity).

The fact that Kocher modifies the DES algorithm, for example by constantly updating the S tables that supply random numbers to the algorithm, in order to keep ahead of an attacker, does not imply that $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$. The reason is as follows: The claimed

invention assumes that the operation used to carry out the encryption will be discovered by an attacker, but seeks to protect the data by using an operation h' whose relationship to the original operation h is random, except that $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$. If the relationship between disguised input data and the original data is not known, then the relationship between h' and h also cannot be discovered. This lack of a predetermined relationship between h' and h, which is what is meant by the term "disguising," has the effect of completely protecting h and x, but also would have the effect of making it impossible to recover the original data even for legitimate reasons if it were not for the claimed relationship $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$. On the other hand, by forcing h' to comply with the relationship $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$, the original data can be recovered without any knowledge of h' at all.

In contrast, Kocher seeks to keep one step ahead of the attacker by varying the various random numbers used in the DES algorithm and adding permutations, and does not seek to disguise the relation between the modified DES algorithm and the so-called "standard DES algorithm." Instead, Kocher assumes that someone seeking to recover the original data can do so in the usual manner, but simply reversing the algorithm applied to the disguised data using secret keys, and then recovering the original data using additional keys (the random numbers used to disguise the data). Kocher does not need the claimed equality (*i.e.*, h_{RI}(disguised input data) = y = h(x)) because, although the "standard" DES algorithm is changed or modified to include different initialization and additional permutations, the DES algorithm is not changed in a random manner. So long as the decryption algorithm used to recover the original data takes into account the modifications made by Kocher to the DES encryption algorithm, there is no need for the claimed equality to hold true.

The logical error made by the Examiner is to assume that the result of encrypting the disguised data using a modified algorithm must equal the result of encrypting the original data using the original algorithm. This is not the case. There are actually many variations of DES, such as DES-X mentioned in paragraph [0068] of the Kocher publication, any of which could be applied to the original or disguised data. There is no reason to assume that a file encrypted

by DES-X would be the same as a file encrypted by DES. If a particular file is encrypted by DES-X, then it must be decrypted by DES-X, and cannot be decrypted by basic DES. Similarly, a file encrypted by Kocher's modified DES, with its additional permutations, will need to be decrypted by a modified version of DES. This is entirely to be expected, and not normally a problem. One does not expect an RSA encrypted file to be identical to a DES encrypted file, and therefore decryptable by the same algorithm. Similarly, one does not expect an encrypted file that has been encrypted by modified DES file to be the same as a file encrypted by DES. The algorithms might be different, but one is not a "disguised" version of the other. So long as the decrypted knows how the file was encrypted, the file can be decrypted, no matter how good the protection against third party attackers. (Note that the same argument applies to decryption, which either requires knowledge of the encryption algorithm, or a decryption algorithm whose output is not affected by the specific algorithm employed, *i.e.*, that exhibits the claimed equality).

Even if one refers to the modified DES algorithm of Kocher as "h'", since h' is merely a modified version of h, someone practicing the teachings of Kocher can simply reverse h' to recover the original disguised data, *i.e.*, to decrypt the encrypted file, and then reverse the data disguising operation to recover the original undisguised data. That is not the case with the claimed invention. Instead, the encryption operation is itself randomized. This does not simply mean that random numbers are used in the operation. All major encryption algorithms use random numbers. Instead, it means that the operation itself has been **modified in a random way**. This is the fundamental difference between the claimed invention and what is taught by Kocher. **The claimed disguising of an operation is not merely modification of the operation (whether by modifying S tables, or adding permutations, or changing the keys), but rather involves a random modification of the operation, necessitating the claimed equality $E(x)_h = E(x')_{h'}$.**

The different nature of the claimed "disguising" of operations and Kocher's teachings concerning variations of the DES algorithm may be further understood from the fact that falsification of the encryption operations, according to the present invention, must be carried

out before execution, *i.e.*, in a safe environment, in order to be able to achieve the claimed equality (*i.e.*, it is necessary to run the disguised operations in order to generate a disguised operation that exhibits the claimed equality). While Kocher's DES modifications do involve initialization, the initialization *changes* each time the algorithm is run, and cannot be carried out in a safe environment by also running the original algorithm. To the contrary, running the unmodified DES algorithm on undisguised data would be contrary to Kocher's goal of varying the initialization or set-up each time a data encryption operation is to be performed and therefore Kocher could not have suggested that the claimed equality between a disguised operation applied to disguised data and an undisguised operation applied to undisguised data.

Conclusion

For all of the foregoing reasons, Appellants respectfully requested reconsideration of the Decision on Appeal, and reversal of final rejection of claims 1-18 under 35 U.S.C. §102(e).

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: July 14, 2008

BACON & THOMAS
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500

S:\Producer\beu\Pending Q...Z\V\WATER 763621\rehearing request.wpd

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of:	)	**Group Art Unit: 2134**
	)	
Harald VATER *et al.*	)	**Examiner: C. Colin**
	)	
Serial Number: 09/763,621	)	***Attorney Docket*: VATE3002beu**
	)	
Filed: April 26, 2001	)	**Confirmation No.: 8124**

For: Access-Protected Data Carrier

REQUEST FOR REHEARING UNDER 37 C.F.R. §41.52
(In Triplicate)

Sir:

This paper is an Request for Rehearing in reply to the Decision on Appeal dated May 13, 2008.

The Appellant believes that the following point raised in the Appeal Brief dated were overlooked or misapprehended by the Board:

- According to page 6 of the Appeal Brief,

  Reversal of the rejection under 35 USC §102(e) is respectfully requested on the grounds that the Kocher publication does not disclose or suggest, whether individually or in common with any other reference of record, a data carrier having a semiconductor chip with a memory and operating program that disguises an operation h and its input x in order to obtain a disguised operation h_{RI} ***different from operation h*** and disguised input data in which:

  $$\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$$

  holds true, *i.e.*, in which **performing the different operation on the disguised input data has the same effect as performing the original operation on the undisguised input data**, as recited in independent claim 1, or in which the result of performing the original operation on the undisguised input data can be determined from the output data with the aid of data used for the disguising the operation, as recited in second independent claim 9.

In the method of Kocher, the relationship $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$ does not hold true.

It appears that the Applicant's arguments concerning "disguising" of the operation have been mis-apprehended. The Board has apparently understood "disguising" to be equivalent to "modifying," which is not the case. The Applicant admits that Kocher modifies the DES algorithm. However, the Applicant does not admit that the modification results in the claimed equality $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$.

In hindsight, it appears that use of the term "standard DES" operation to describe Kocher's modified DES algorithm may have confused the Board (and the Examiner). It actually does not matter whether the DES operation described by Kocher should be considered to be "standard" or not. The critical point, which has been misapprehended or overlooked, is that Kocher does not seek to achieve the relationship $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$, and in fact does not require such a relationship. Just because Kocher modifies the "standard" DES algorithm does not mean that the result of applying of the modified DES algorithm to disguised input data (M1,M2 according to Kocher's terminology) is exactly equal, as claimed, to the result of applying the "standard" DES algorithm to the undisguised input data (M). To the contrary, there is no inherent reason why there should be any relationship between applying an encryption (or decryption) algorithm to data and applying a modified encryption (or decryption) algorithm to either the same data, a disguised version of the data, or entirely different data.

Kocher is not the only one to teach modifications to the DES algorithm, and it is hardly reasonable to expect that all of such modifications will obey the claimed equality. For example, as explained below, Kocher mentions that the modifications made to the DES algorithm (revised initialization procedures and added permutations) could also be applied to DES-X, or even to RSA. It is not reasonable to expect that the result of applying the revised DES-X or RSA algorithms to disguised data M1,M2 would be equal to the result of applying standard DES to original data M. Instead, the result will be different each time a modification is made to DES,

unless the modifications are specifically designed, as in the claimed invention, to obtain the same result, *i.e.*, the claimed equality $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$.

This is not a repeat of the arguments made in the Appeal Brief, but it also is not a new argument. It appears that there has been a mis-understanding of Applicant's arguments based on semantics (*i.e.*, unfortunately choice of terminology on the part of the undersigned, which seems to have caused confusion). In particular, Applicant's use of the term "standard" to describe Kocher's modified DES algorithm was unfortunate. Kocher in fact clearly does modify the DES algorithm, by varying the initialization process for the S tables and by adding permutations and varying the keys. What the Board/Examiner has overlooked, and the Appeal Brief apparently did not make completely clear, is that modifying is not the same as disguising.

The Applicant's "disguising" operation is actually a randomizing operation, and not just randomization by inputting random numbers. Applicant's "disguising: operation actually results in an operation that does not bear a predetermined relationship to the original operation, *which is why it is necessary that* $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$. If the claimed equality were not present, then it would be impossible (or at least extremely difficult) for a decrypter to recover the original data (or for en encrypter to encrypt the data in a way that could be recovered) because the operation used to encrypt the data has been "**disguised**" and **not merely modified**. This is a fundamental feature of the claimed invention, which relies on the lack of a predictable relationship between the original algorithm and the disguised algorithm to protect the original algorithm. Kocher's goal is completely different, namely to modify DES in such a way as to make it more difficult to detect *during execution*. Kocher does not seek to hide the manner in which the DES algorithm has been modified, and therefore does not require a relationship between the original and modified algorithms, as claimed.

What has been misapprehended is that the claimed "disguised operation" is not at all the same as Kocher's modified DES operation. While use of the term "disguised" might by itself

not distinguish the claimed invention from a modified algorithm as taught by Kocher, the term "disguised" was intended to have an entirely different meaning than "modified." The difference is that a disguised operation cannot be reversed, with the result that it is necessary to impose an additional equality, namely that $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$, which is not at all necessary if the operation is merely modified as in Kocher.

The claimed invention has two aspects: a. disguising of data; and b. disguising of operations to be performed on the data. The Kocher publication clearly teaches disguising of input data and keys (see paragraphs [0033] to [0037]), and in fact uses the same disguising operation as Applicant. In particular, input data M is disguised by X-ORing with a random number to obtain M1 and M2 (M1 is the random number and M2 is the X-OR'd random number). Key K is also disguised by X-ORing with a random number. This is the same basic process as is used by the present invention to disguise the input data (both the "message" and the "keys" are input data).

Further, it is absolutely true that Kocher teaches ***modifications*** to the DES algorithm. These modifications involve improving the manner in which the S tables are initialized and updated so that the table entries can be changed more frequently (preferably the table entries are changes faster than they can be discovered by an attacker), as described in paragraphs [0039] to [0051]. In addition,"improvements" or modifications to the DES algorithm are described in paragraphs [0052] to [0064]. These modifications involve adding permutations, such as the PC2 operation in paragraph [0054], which is apparently a departure from the "standard DES PC1 operation" described in the first sentence of the paragraph. The result is a modified DES algorithm which has harder-to-discover random number inputs, resulting from improved *initialization* of the S tables, and more permutations (both in quantity and complexity).

The fact that Kocher modifies the DES algorithm, for example by constantly updating the S tables that supply random numbers to the algorithm, in order to keep ahead of an attacker, does not imply that $\mathbf{h_{RI}(disguised\ input\ data) = y = h(x)}$. The reason is as follows: The claimed

invention assumes that the operation used to carry out the encryption will be discovered by an attacker, but seeks to protect the data by using an operation h' whose relationship to the original operation h is random, except that $\mathbf{h_{RI}}$**(disguised input data) = y = h(x)**. If the relationship between disguised input data and the original data is not known, then the relationship between h' and h also cannot be discovered. This lack of a predetermined relationship between h' and h, which is what is meant by the term "disguising," has the effect of completely protecting h and x, but also would have the effect of making it impossible to recover the original data even for legitimate reasons if it were not for the claimed relationship $\mathbf{h_{RI}}$**(disguised input data) = y = h(x)**. On the other hand, by forcing h' to comply with the relationship $\mathbf{h_{RI}}$**(disguised input data) = y = h(x),** the original data can be recovered without any knowledge of h' at all.

In contrast, Kocher seeks to keep one step ahead of the attacker by varying the various random numbers used in the DES algorithm and adding permutations, and does not seek to disguise the relation between the modified DES algorithm and the so-called "standard DES algorithm." Instead, Kocher assumes that someone seeking to recover the original data can do so in the usual manner, but simply reversing the algorithm applied to the disguised data using secret keys, and then recovering the original data using additional keys (the random numbers used to disguise the data). Kocher does not need the claimed equality (*i.e.*, h_{RI}(disguised input data) = y = h(x)) because, although the "standard" DES algorithm is changed or modified to include different initialization and additional permutations, the DES algorithm is not changed in a random manner. So long as the decryption algorithm used to recover the original data takes into account the modifications made by Kocher to the DES encryption algorithm, there is no need for the claimed equality to hold true.

The logical error made by the Examiner is to assume that the result of encrypting the disguised data using a modified algorithm must equal the result of encrypting the original data using the original algorithm. This is not the case. There are actually many variations of DES, such as DES-X mentioned in paragraph [0068] of the Kocher publication, any of which could be applied to the original or disguised data. There is no reason to assume that a file encrypted

by DES-X would be the same as a file encrypted by DES. If a particular file is encrypted by DES-X, then it must be decrypted by DES-X, and cannot be decrypted by basic DES. Similarly, a file encrypted by Kocher's modified DES, with its additional permutations, will need to be decrypted by a modified version of DES. This is entirely to be expected, and not normally a problem. One does not expect an RSA encrypted file to be identical to a DES encrypted file, and therefore decryptable by the same algorithm. Similarly, one does not expect an encrypted file that has been encrypted by modified DES file to be the same as a file encrypted by DES. The algorithms might be different, but one is not a "disguised" version of the other. So long as the decrypted knows how the file was encrypted, the file can be decrypted, no matter how good the protection against third party attackers. (Note that the same argument applies to decryption, which either requires knowledge of the encryption algorithm, or a decryption algorithm whose output is not affected by the specific algorithm employed, *i.e.*, that exhibits the claimed equality).

Even if one refers to the modified DES algorithm of Kocher as "h'", since h' is merely a modified version of h, someone practicing the teachings of Kocher can simply reverse h' to recover the original disguised data, *i.e.*, to decrypt the encrypted file, and then reverse the data disguising operation to recover the original undisguised data. That is not the case with the claimed invention. Instead, the encryption operation is itself randomized. This does not simply mean that random numbers are used in the operation. All major encryption algorithms use random numbers. Instead, it means that the operation itself has been **modified in a random way**. This is the fundamental difference between the claimed invention and what is taught by Kocher. **The claimed disguising of an operation is not merely modification of the operation (whether by modifying S tables, or adding permutations, or changing the keys), but rather involves a random modification of the operation, necessitating the claimed equality $E(x)_h = E(x')_h$.**

The different nature of the claimed "disguising" of operations and Kocher's teachings concerning variations of the DES algorithm may be further understood from the fact that falsification of the encryption operations, according to the present invention, must be carried

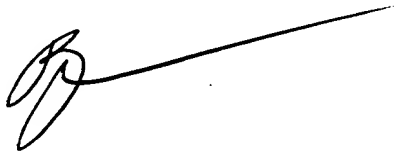
out before execution, *i.e.*, in a safe environment, in order to be able to achieve the claimed equality (*i.e.*, it is necessary to run the disguised operations in order to generate a disguised operation that exhibits the claimed equality). While Kocher's DES modifications do involve initialization, the initialization *changes* each time the algorithm is run, and cannot be carried out in a safe environment by also running the original algorithm. To the contrary, running the unmodified DES algorithm on undisguised data would be contrary to Kocher's goal of varying the initialization or set-up each time a data encryption operation is to be performed and therefore Kocher could not have suggested that the claimed equality between a disguised operation applied to disguised data and an undisguised operation applied to undisguised data.

Conclusion

For all of the foregoing reasons, Appellants respectfully requested reconsideration of the Decision on Appeal, and reversal of final rejection of claims 1-18 under 35 U.S.C. §102(e).

Respectfully submitted,

BACON & THOMAS, PLLC



By: BENJAMIN E. URCIA
Registration No. 33,805

Date: July 14, 2008

BACON & THOMAS
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500

S:\Producer\beu\Pending Q...Z\VV\VATER 763621\rehearing request.wpd